The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method of communicating state information between a server and a client having a memory, the method comprising the steps of:

i) providing an asymmetric encryption method having a public key provided to said client and said server and a private key provided to said server;

ii) said client communicating a client request to said server to perform a server action;

iii) said server responsive to receiving said client request, performing said server action and creating a state object containing post-action state information;

iv) encrypting said state object using said private key;

v) communicating said encrypted state object and a result of said server action to said client; and

vi) storing said encrypted state object in said client memory.

2. A method according to claim 1, further comprising the steps of:

vii) said client communicating a subsequent client request to said server to perform a server action and said server receiving from said client said encrypted state object with said subsequent client request; and

viii) said server, responsive to receiving the subsequent client request, decrypting said received encrypted state object using said public key.

3. The method according to claim 2, further comprising the step of:

ix) said server, after decrypting said received encrypted state object, verifying whether said received state object has been modified.

4. The method according to claim 1 wherein said server is stateless and said client is stateful.

5. The method according to claim 1 comprising the further step of said client decrypting said state object using said public key.

6. The method according to claim 3, said method comprising the further steps of:

x) said server, after verifying that said received state object has not been modified, using state information contained therein to perform the requested action;

xi) responsive to performing the requested action, replacing previous state information with new state information in said state object;

xii) encrypting said state object with said private key; and

xiii) sending said encrypted state object and a result of said server action to the client.

7. A data processing system for communicating state information between a server and a client having a memory, said data processing system comprising:

i) means for receiving a client request to perform a server action;

ii) means, responsive to said client request receiving means, for performing said server action and creating a state object containing post-action state information;

iii) means for encrypting said state object comprising an asymmetric encryption method having a public key provided to said client and said server and a private key provided to said server; and

iv) means for communicating said encrypted state object and a result of said server action to said client.

8. A data processing system according to claim 7, further comprising:

v) means for receiving from said client said encrypted state object with a subsequent client request to perform a server action;

vi) means, responsive to said means for receiving said subsequent client request, for decrypting said received encrypted state object using said public key; and

vii) means for verifying whether said received state object has been modified.

9. A data processing system according to claim 8, further comprising:

viii) means, responsive to said verifying means, for using state information contained in said state object to perform said requested server action;

vi) means for replacing previous state information with new state information in said state object;

vii) means for encrypting said state object using said private key; and

viii) means for sending said encrypted state object and a result of said server action to said client.

10. The data processing system according to claim 9 further comprising means for receiving said encrypted state object; means for decrypting said state object using said public key; and means for storing said encrypted state object.

11. A computer program product for communicating state information between a server and a client having a memory, said server provided with a public key and a private key of an asymmetric encryption method and said client provided with a public key of an asymmetric encryption method, said computer program product comprising:

a computer usable medium having computer readable program code means embodied in said medium for receiving a client request to perform a server action;

said computer usable medium having computer readable program code means embodied in said medium, responsive to said client request receiving means, for performing said server action and creating a state object containing post-action state information;

said computer usable medium having computer readable program code means embodied in said medium for encrypting the created state object with the private key of said asymmetric encryption method; and

said computer usable medium having computer readable program code

means embodied in said medium, responsive to said encrypting means, for sending said encrypted state object and a result of said server action to said client.

12. A computer program product according to claim 11, further comprising:

computer readable program code means embodied in said medium for receiving from said client said encrypted state object with a subsequent client request to perform a server action;

computer readable program code means embodied in said medium, responsive to said means for receiving the subsequent client request, for decrypting said received encrypted state object using said public key; and

computer readable program code means embodied in said medium, responsive to said decrypting means, for verifying that the received state object whether said received state object has been modified.

13. A computer program product according to claim 12, further comprising:

computer readable program code means embodied in said medium for replacing previous state information with new state information in said state object;

computer readable program code means embodied in said medium for encrypting said state object using said private key; and

computer readable program code means embodied in said medium for sending said encrypted state object with said new state information and a result of said server action resulting from said subsequent client request to said client.

14. A computer program product for communicating state information between a server and a client having a memory, said server provided with a public key and a private key of an asymmetric encryption method and said client provided with a public key of an asymmetric encryption method, said computer program product comprising:

a computer usable medium having computer readable program code means embodied in said medium for sending a client request to perform a server action;

said computer usable medium having computer readable program code means embodied in said medium for receiving the results of said server action and a state object containing post-action state information wherein said state object is encrypted with said private key of said asymmetric encryption method, and means for storing said state object; and

said computer usable medium having computer readable program code means embodied in said medium for decrypting said state object with the public key of said asymmetric encryption method.